

A Novel Method for Soft Error Mitigation in FPGA using Adaptive Cross Parity Code

Swagata Mandal^{*}, Rourab Paul[†], Suman Sau[‡], Amlan Chakrabarti[§] and Subhasis Chattopadhyay[¶]
^{*}{swagata.mandal^{*}, sub[¶]}@vecc.gov.in^{*}, [†]{rpakc_sl[†], ssakc_sl[‡], acakcs1[§]}@caluniv.ac.in[¶]
 Variable Energy Cyclotron Center, Saltlake, Kolkata, India^{*}, University of Calcutta, Kolkata, India^{†‡§}

Abstract—Field Programmable Gate Arrays (FPGAs) are more prone to be affected by transient faults in presence of radiation and other environmental hazards compared to Application Specific Integrated Circuits (ASICs). Hence, error mitigation and recovery techniques are absolutely necessary to protect the FPGA hardware from soft errors arising due to such transient faults. In this paper, a new efficient multi-bit error correcting method for FPGAs is proposed using adaptive cross parity check (ACPC) code. ACPC is easy to implement and the needed decoding circuit is also simple. In the proposed scheme total configuration memory is partitioned into two parts. One part will contain ACPC hardware, which is static and assumed to be unaffected by any kind of errors. Other portion will store the binary file for logic, which is to be protected from transient error and is assumed to be dynamically reconfigurable (Partial reconfigurable area). Binary file from the secondary memory passes through ACPC hardware and the bits for forward error correction (FEC) field are calculated before entering into the reconfigurable portion. In the runtime scenario, the data from the dynamically reconfigurable portion of the configuration memory will be read back and passed through the ACPC hardware. The ACPC hardware will correct the errors before the data enters into the dynamic configuration memory. We propose a first of its kind methodology for novel transient fault correction using ACPC code for FPGAs. To validate the design we have tested the proposed methodology with Kintex FPGA. We have also measured different parameters like critical path, power consumption, overhead resource and error correction efficiency to estimate the performance of our proposed method.

I. INTRODUCTION

Soft errors, also known as transient errors are temporary malfunction occur in solid state device due to the radiation. They are not reproducible [1] and sometimes leads to single event upset (SEU). With the development of fabrication technology, solid state devices are gradually reducing in size. Due to this downscaling in device size, node voltage of CMOS transistors are also reducing. Generally if the charge injected by these particles are above certain threshold (also known as critical charge [2]) they can create SEU in different embedded devices like FPGA. Meanwhile demand of FPGAs are gradually increasing in different critical applications like High energy physics experiment, biomedical instrumentations, deep space exploration *etc* due to its different advantages over ASICs. So different fault mitigation techniques are required to protect these FPGA devices from radiation and energetic particles.

Errors in FPGA can be broadly classified into two main categories: Temporary or transient error and permanent error [3]. Transient error may create SEU into any combinational or sequential logic, which will be transferred to the flipflop or

memory. But this error can be corrected within a few seconds. Sometimes transient error may directly affect configuration memory of FPGA. This error can not be corrected unless we re-configure the FPGA. This is also one kind of permanent fault but it is recoverable. Sometimes it may also happen that the charge particles permanently damage the logic or switching block within the FPGA. This error can be sorted out only by replacing the logic block physically (normally it is done by routing [4]). In our work, we considered permanent recoverable faults only.

One of the common solution to prevent from radiation effect is to use radiation hardened (Radhard) FPGAs like space grade FPGA. But they are more costly compared to the commercial-off-the-shelf (COTS) FPGA [5]. These Radhard FPGAs are also few generation behind than COTS FPGAs. Available memory within the FPGAs can be classified into four categories [6]: Configuration Memory, Block Memory, Distributed Memory, Flip-Flops. Out of these, Block memory, Distributed memory and Flip-Flops store the user logic. Configuration memory store the data related to configuration of the user logic. Normally, it is assumed that after downloading the bit file into the configuration memory it should remain unchanged while user logic in other memory can change any time with the clock cycle. Within the FPGA most of the memory bits are configuration bits. So the probability of occurrence of error is more in configuration memory. But, the common error correcting technology like tripple modular redundancy (TMR) [7], Concurrent error detection (CED) [8] are used for user logic not for configuration memory. Apart from this, above mentioned schemes also consume large area, huge power and are not suitable for real time applications. Large area overhead of TMR can be reduced by using TMR only in critical portion of a circuit instead on the whole design which is known as partial TMR as described in [9]. The problem related to extra overhead can be reduced by using different technologies like scrubbing and various error detection and correction codes (EDAC).

In this paper the key contributions are:

- A novel technique for error detection and correction using adaptive cross parity code (ACPC) is adopted to protect the configuration memory from soft error. The optimized ACPC architecture consumes very less resource and power compared to the remaining logic.
- ACPC mounted custom architecture of Internal Configuration Access Port (ICAP) Intellectual Property (IP) is proposed where bit file reading, fault detection, fault correction and writing process are pipelined to increase the throughput.

- The partial reconfiguration feature in proposed fault correction module reduces reconfiguration time and produces a worst case solution when the number of faults exceeds fault correction capacity .

The rest of the paper is organized as follows. Section II presents a detailed literature review related to our work and section III describes proposed the ACPC code in details. Proposed hardware architecture is described in section IV. Performance evaluation with result analysis is described in section V followed by concluding remarks in section VI.

II. BACKGROUND AND RELATED WORK

Scrubbing is the best alternative solution to mitigate the effect of soft error without any extra area overhead like TMR and CED. In scrubbing, during download of the bit file into the configuration memory, one copy of original bit file (also known as golden copy) is stored separately in a Radhard memory. During run time, this golden copy is downloaded into configuration memory with some periodic interval. It reduces the effect of accumulated error in FPGA and increases the lifespan of the FPGA [10]. An alternative to this method is known as configuration read back as described in [3]. In this scheme data from the configuration memory is continuously read back and cyclic redundancy checking (CRC) operation is done in a separate radiation hardened memory. After detecting the error FPGA has to be re-programmed again. Sometimes TMR can also be used intelligently with scrubbing to reduce the effect of single event upset as described in [11] for Virtex FPGAs. Both of the above mentioned schemes have some drawbacks as they have to continuously access some external radhard memory, which increases the cost and introduces some delay.

To reduce the delay, a part of the bit file can be downloaded during scrubbing without downloading the whole one. Authors in [12] use partial reconfiguration with scrubbing to reduce the effect of delay. Partial reconfiguration can also be used to reduce the effect of SEU. In this case the portion where error is detected, only that portion will be corrected. But during the correction whole system has to be stopped for a moment. This can not be the good solution for real time systems. In [13], the authors used dynamic partial reconfiguration to correct only a portion of the configuration memory, which is affected by soft errors without hampering the function of the rest of the configuration memory.

Another approach is to use the EDAC codes or cyclic redundancy checking (CRC) to protect the configuration memory without any extra hardware or without any extra delay. Normally, the error correcting codes are used in communication domain. One of the main parameter for the performance analysis of the EDAC in communication domain is it's closeness to shannon limit [14]. To support real time requirements EDAC with less complex decoding circuit is preferred. In [15] the authors used 2-D hamming product code to correct multi-bit upset (MBU) in each configuration frame. They also proposed one special kind of memory as hardware implementation of their proposed code is tough in the conventional configuration memory. Xilinx itself provides soft error mitigation controller (IP blocks) which is based on both CRC and EDAC. This IP can correct atmost two adjacent bits [6]. Present studies [16]

show that faster rate of downscaling cause multiple number of adjacent bits to be affected by radiation. So more complex EDAC is required to mitigate the effect of soft error. Authors use convolutional code to mitigate the effect of SEU in [17]. Main problem of the convolutional coding is that the decoding circuit is very complex.

With the reduction of the complexity of the decoding circuit usefulness of EDAC will increase in SEU mitigation. Now a days different parity check codes are used intelligently in MBU correction. *Parthasarathy et.al* use interleaved parity check code along with scrubbing against MBU in SRAM based FPGA in [18].

III. PROPOSED ADAPTIVE CROSS PARITY CHECK CODE ALGORITHM AND ARCHITECTURE

A class of parity code, Cross Parity Check Code is very useful for protecting the data stored in configuration memory of FPGA against transient errors. ACPC code was first proposed in [19] for correcting errors in magnetic tapes. Error correcting procedure in magnetic tape is quite different from SRAM based FPGA. To use ACPC code for correcting fault in SRAM based FPGA, a portion of ACPC code is modified. This modification helps to correct any odd number of errors along either positive or negative slope in configuration memory. Coding structure of ACPC is very simple because it does not use complex computation of Galois field unlike other commonly used error correcting code like Bose Choudhury Hocquenghem (BCH) code and Reed Solomon (RS) code. It also avoids decoding circuit complexity as in LDPC and Turbo codes. It is clearly evident from the data presented in Table I, that the proposed ACPC code gives better performance in terms of decoding circuit complexity, latency and hardware complexity as compared to the other state of the art codes. Here a 7x7 matrix is chosen to measure code rate as shown in Table I. Code rate for turbo code and LDPC are not shown in the Table I, as it is not a standard parameter to measure coding efficiency for these classes of codes. Binary file for logic design will be stored in a matrix format in configuration memory. In this paper to show the use of the proposed modified ACPC code we have chosen only a part of the configuration memory in a 18x17 matrix as shown in Figure 1. However it is easy to extend the result with any other size of the matrix.

In this coding scheme the concept of interacting vertical and cross parity checks are used in an adaptive manner. Before entering into the encoding process, 18x17 matrix is divided into two matrices M1 and M2 of size 9x17. Then rows of M1 and M2 are interleaved. After interleaving new row number is assigned along a column in the left side of the matrix. Vertical checking can be applied independently in two matrices but cross parity checking is spanned over two matrices at the same time. The decoding process is iterative and based on parity equation, which contains one variable at a time. This makes the decoding process simple and inexpensive. Details of encoding and decoding process are described in subsection III-A and III-C respectively.

A. Encoding Process

Let $M1(t)(m)$ and $M2(t)(m)$ indicate m^{th} bit in t^{th} row in matrix M1 and M2 respectively. Row number t can vary from 0 to 8 and m can vary from 0 to 16 in each matrix. Row 0 and 8 in each matrix are used to store the check bit. Row 0

TABLE I. COMPARISON BETWEEN PROPOSED EC SCHEME WITH OTHER EXISTING EC SCHEME

	Block Code		Convolutional Code		Product Code		Cross Parity Code
	Reed-Solomon	Hamming Code	LDPC	Turbo	Reed-Solomon Product	2D Product Code	Proposed ACPC
Hardware Complexity	Moderate	Low	High	High	Moderate	Low	Low
ECC performance	Moderate	Low	Near Shanon Limit	Near Shanon Limit	very strong	strong	strong
Latency	Low	Very Low	Moderate	Long	Very Long	Moderate	Low
Decoding Complexity	Moderate	Low	High	High	High	Low	Low
Code rate	0.467	0.57	N/A	N/A	0.3	0.285	0.35

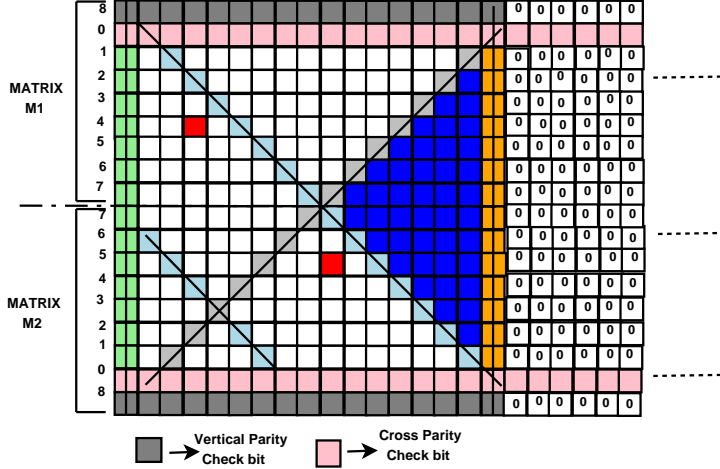


Fig. 1. Data Format for a part of a configuration memory

of matrix M1 stores the cross parity check bit for the diagonal with positive slope for bit from M1 and M2. So m^{th} bit of 0^{th} row can be calculated as:

$$M1(0)(m) = \sum_{t=1}^7 M1(t)(m-t) \oplus \sum_{t=0}^7 M2(t)(m+t-15)$$

Similarly 0^{th} row of matrix M2 stores the cross parity check bit for the diagonal with negative slope for M1 and M2. So m^{th} bit of 0^{th} row can be calculated as;

$$M2(0)(m) = \sum_{t=1}^7 M2(t)(m-t) \oplus \sum_{t=0}^7 M1(t)(m+t-15)$$

At the beginning of the encoding process each check bit value is set to 0. A certain portion of the 18x17 matrix (indicated by blue color in Figure 1) remain uncoded in the above mentioned coding scheme. So some extra portions of the memory is added in the right side of the matrix. In this extra portion of the memory, rows for cross parity bit will be used and remaining portions are loaded with zero value. The check bits in the 8^{th} row of each matrix are generated from the parity equation along the column of each matrix. So the m^{th} check bit in the 8^{th} row of matrix M1 can be generated from the following equations

$$M1(8)(m) = \sum_{t=0}^7 M1(t)(m)$$

$$M2(8)(m) = \sum_{t=0}^7 M2(t)(m)$$

B. Syndrome Computation

Let $\hat{M}1(t)(m)$ and $\hat{M}2(t)(m)$ denote the corrupted bits obtained after reading the configuration memory during the run time from t^{th} row and m^{th} column of M1 and M2 matrices respectively. Non zero syndrome value will indicate the presence of error, so syndrome for m^{th} bit in the t^{th} row of M1 matrix is:

$$Xd_m^{M1} = \sum_{t=0}^7 \hat{M}1(t)(m-t) \oplus \hat{M}2(t)(m+t-15)$$

Similarly, syndrome for m^{th} bit in the t^{th} row of M2 matrix is:

$$Xd_m^{M2} = \sum_{t=0}^7 \hat{M}2(t)(m-t) \oplus \hat{M}1(t)(m+t-15)$$

Syndrome for vertical check at m^{th} column for matrix M1 and M2 are (as shown by yellow color in Figure 1)

$$Xv_m^{M1} = \sum_{t=0}^8 \hat{M}1(t)(m); Xv_m^{M2} = \sum_{t=0}^8 \hat{M}2(t)(m)$$

Modulo two addition between original data and data read back from the memory during the runtime gives the error pattern. So for error pattern of m^{th} bit in the t^{th} row in matrices M1 and M2 are:

$$E(t)_m^{M1} = \hat{M}1(t)(m) \oplus M1(t)(m)$$

$$E(t)_m^{M2} = \hat{M}2(t)(m) \oplus M2(t)(m)$$

So, the syndrome vectors can be written in terms of error pattern as follows:

$$Xd_m^{M1} = \sum_{t=0}^7 E(t)_m^{M1} \oplus E(t)_m^{M2}$$

$$Xd_m^{M2} = \sum_{t=0}^7 E(t)_m^{M2} \oplus E(t)_m^{M1}$$

$$Xv_m^{M1} = \sum_{t=0}^8 E(t)_m^{M1}; Xv_m^{M2} = \sum_{t=0}^8 E(t)_m^{M2}$$

C. Decoding Process

Decoding process consists of two steps: 1) Detection of the erroneous bits in the Matrix 2) Correction of the detected erroneous bits. Before starting of the decoding process, data from the configuration memory will be read back and store within the decoder circuit. Decoding obeys the following steps:

Input: Read M1 and M2;

Output: Corrected bit value and corrected bit position;

Step1: Set vertical pointer m=2;

Step2: Set the pointer along the positive slope as U = 1 and set the pointer along the negative slope as W=14;

Step3: Increase the pointer along the positive slope and perform the modulo two sum between the elements obtained along the positive slope;

Step4: After reaching the first row perform the modulo two sum between the result obtained in the previous step and parity value in the 0^{th} row in M1;

Step5: Increase the pointer along the negative slope and perform the modulo two sum between the elements obtained along the negative slope.

Step6: After reaching the 14^{th} row perform the modulo two sum between the result obtained in the previous step and the parity value in the 0^{th} row of M2.

Step7: Nonzero modulo two sum at step 4 or step 6 indicates the presence of error along that positive or negative slope respectively. Zero modulo two sum indicates either there is no error or our coding is unable to detect the error.

Step8: After getting nonzero modulo sum one pointer starts

from first column for the process with positive slope and move horizontally. For each increment it will perform the modulo sum along the vertical direction.

Step9: Similarly, after getting nonzero modulo sum one pointer starts from first column for the process with negative slope and moves horizontally. For each increment it will perform the modulo sum along the vertical direction.

Step10: Step 8 and Step 9 will continue until non zero syndrome is obtained along the vertical direction. The position where syndrome is nonzero along the vertical direction gives the exact position of the error.

Step11:After getting the error it can be corrected by simple inversion.

Step12: The process will continue until all errors along the diagonal are corrected. Next, step 3 to step 11 will continue for all the errors in the whole matrix.

Proposed coding scheme can maximally correct two errors along any column if they are in two halves *i.e* one is in M1 and other will be in M2 and any odd number of errors along the diagonal. In a column of a $n \times n$ window, the number of correctable 2 bit faults can exist in two halves is $\frac{n}{2} \times \frac{n}{2}$. Hence, the number of undetectable faults are $2^n - 1 - (\frac{n}{2} \times \frac{n}{2})$ which can be expressed by:

$$C_u = n! \int_{i=3}^n \frac{1}{(n-i)! \times i!} + 2 \times \frac{n}{2} C_2$$

The possible number of successive diagonal faults are

$$D_t = 2(n! \int_{i=2}^n \frac{1}{(n-i)! \times i!} + 2 \int_{i=2}^n \frac{1}{i!} \int_{j=n-1}^i (n-i) \prod_{k=i}^n (j-k))$$

The proposed algorithm can correct $\frac{D_t}{2}$ number faults. Hence, the fault correcting efficiency for successive diagonal bits are 50%. Proposed code can correct any number of errors along the row. The advantages of the proposed coding scheme are: 1) In the proposed coding scheme two process run in parallel. One is along the positive diagonal and the other is along negative diagonal. This will enhance the speed of the decoding process.

2) The coding process is adaptive in nature. Error corrected in one bit position will help error correction at other positions too. This can be described as follows:

Suppose there are two errors in M1 and M2 indicated by red color in Figure 1. If only process related to negative slope will run then they can not be detected because they are on the same diagonal. But if the process related to positive slope also runs, error in M1 will be corrected first and then it is possible to correct error in M2 using the process along negative slope.

IV. HARDWARE ARCHITECTURE

A. Configuration Area

Application hardware, placed into configuration area of FPGA chip consists few sub-components, which may be stated as standard IP or custom IPs. In this architecture each component takes one partitioned area of the FPGA. The Fault correcting block (ACPC) reads binary file (bit file) of the whole Application hardware through the ICAP ports. ACPC block corrects the faulty bits and stores addresses of

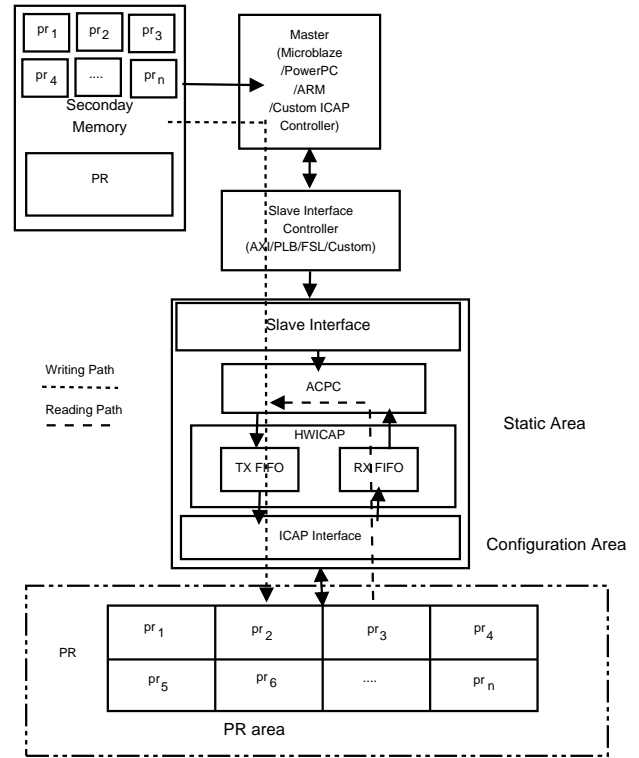


Fig. 2. Architecture of proposed ICAP block

the partition regions where faults were occurred. While the whole bit scanning is done, ACPG sends only the bit files of faulty partitions to ICAP. It is to be noted that partitioning for each component is needed to reduce reconfiguration time otherwise whole bit file downloading process may take more reconfiguration time.

B. Proposed ICAP block

The proposed ICAP block consists of 3 sub blocks, slave interface, ACPC block and Hardware ICAP (HWICAP) as shown in Figure 2.

1) *Slave Interface::* Slave interface of ICAP gets the controlling information from master. Master sends two important informations namely ICAP_start, and bit length. ICAP acknowledges master using ICAP_done port while dynamic configuration process is done. In Xilinx platform we can use Microblaze, power PC, arm or custom ICAP controller as a master.

2) *ACPC Block*:: Detail hardware architecture of ACPC block is described in section III. ACPC is connected with HWICAP IP provided by Xilinx. ACPC can read or write bit file information from read and write buffer of HWICAP respectively.

3) **HWICAP::** The HWICAP is an interface to the Internal Configuration Access Port (ICAP). The write FIFO inside HWICAP stores the configuration bit locally. The master writes the configuration bit into to the write FIFO. Simultaneously, the data stored in the write FIFO is transferred to the ICAP. The master reads the configuration data from the ICAP stored inside the read FIFO. FIFOs are used because the rate of data flow from the master interface is different from the ICAP interface. FIFO depth is flexible.

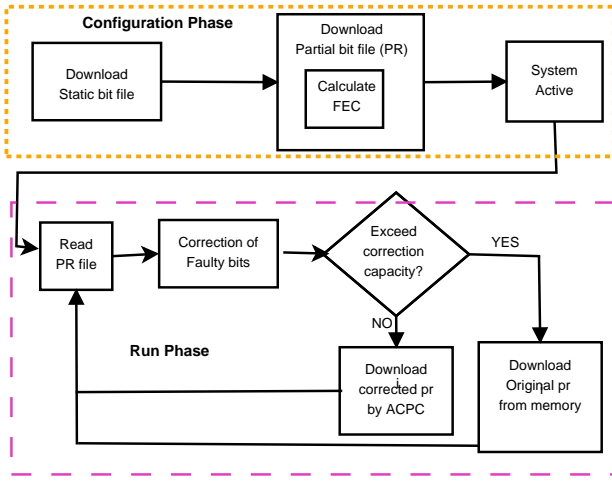


Fig. 3. Workflow during hardware implementation of our proposed Algorithm

C. Slave Interface Controller

Slave interface controller is an interface between proposed ICAP block and master. The master processing element can send partial bit files from secondary memory to proposed ICAP block. The type of slave interface controller depends on master. If the master is standard processor like Microblaze, Power PC or ARM then this interface must follow the standard bus protocol. AXI, FSL and PLB are the options to serve the communication between standard processor and proposed ICAP block. The interface will be custom if custom ICAP controller processor is used as master.

D. Master ICAP Controller and Secondary memory

Master ICAP Controller is used to move partial bit files from secondary memory to proposed ICAP controller. Microblaze, Power PC, ARM or custom light weight ICAP controller can be used as the master. Flash or Secure Disk (SD) card can be used as secondary memory to store bit files.

E. Workflow

The whole design is separated into static and partial region. Static portion consists of secondary memory, master processor, slave bus interface and the proposed ICAP block. The partial region only contains the application hardware. The work flow of the proposed design is described below:

Step1: Only the static bit file is downloaded in the configuration area of the FPGA through JATG cable from secondary memory.

Step2: The partial bit file of the whole application named as PR is stored in the secondary memory along with sub-components bit files as shown in Figure 2. Here $PR = pr_1 + pr_2 + pr_3 + \dots + pr_i + \dots + pr_N$.

Step3: The PR bit file is now downloaded into the partitioned partial region through the proposed ICAP block. During this pass, ACPC inside the ICAP block calculates the forward error correction (FEC) field.

Step5: After a specified time interval ICAP starts to read the PR file. If fault occurs, ACPC corrects the specific bits and re-downloaded corresponding pr_i (i from 1 to N) files in the allocated partitions. If the number of faulty bit exceeds form correction capacity of ACPC, the ICAP will request master to re-download the whole pr_i file from the secondary memory. We demarcate two distinct phases in the wokflow namely,

TABLE II. RESOURCE UTILIZATION BY THE PROPOSED DESIGN

Block name	# Slice	# LUT -FF Pair	Critical time(ns)	Power (mw)
Encoder	1052	1012	2.3137	10.8
Decoder	1759	1650	1.774	15.7
Gaussian	4508	4042	-	1260
RC4	5383	-	-	994

configuration phase and run phase as illustrated in Figure 3. Step 1-3 describes the configuration phase and step 4 describes the run phase.

V. RESULTS AND PERFORMANCE ANALYSIS

Our fault correcting model is implemented on the Xilinx Kintex 7 boards using Xilinx ISE 14.5 platform and VHDL for design entry. An application design is used to generate the bit file. We have tested our design using behavioral simulation. Timing diagram of different signals used in the simulation are shown in Figure 4.

Before starting of encoding process, the bit file will come into ACPC hardware from the secondary storage. When **Enc_start** signal goes high encoding process will start. In the next clock cycle parity checking procedure will be started. In this step parity is calculated along positive and negative slope and along the vertical direction as described in section III. After completion of the encoding process **Enc_Done** signal goes high and the generated redundant data during encoding process will be stored within the ACPC hardware. During the decoding process bit file from the configuration memory will be read back and stored into the ACPC hardware. At the starting of the decoding process **Decode_start** signal goes high and from the next clock cycle syndrome calculation will be started when **Dia_syn** goes high. When non zero syndrome will come syndrome calculation will be stopped as **Dia_syn** signal goes low. At the same instant **syn_nonzero** signal goes high and **varticle_syn** goes low indicate the calculation of syndrome along the vertical direction. When non zero syndrome will be generated along the vertical direction **Error_detect** goes high to indicate that the error is detected. At the next clock cycle **Error_correct** signal will be high for one clock cycle where detected error will be corrected. This process will continue until all errors along a slope will be corrected. After rectification of errors along one slope **Dia_syn** signal will again go high to indicate the repetition of the process along other slope. After completion of error correction along all diagonals **decode_done** signal will go high to indicate the end of the process. After error correction, the region where error is occurred will be downloaded into the configuration memory instead the whole bit file. This will reduce the time and complexity.

All encoding and decoding processes along the slope and vertical direction will run in parallel. This enhances speed of the error correction. To accelerate the encoding and decoding process further, proposed error correcting code can use pipe line architecture during the read write operation in memory through ICAP. But the problem is that in ICAP only one port is available for read and write operation. So we have to do it serially. After error correction on one copy of the bit file, the position of the occurrence of error and corrected value in that position will be stored in the ACPC hardware. In the next time before starting of the error correction on

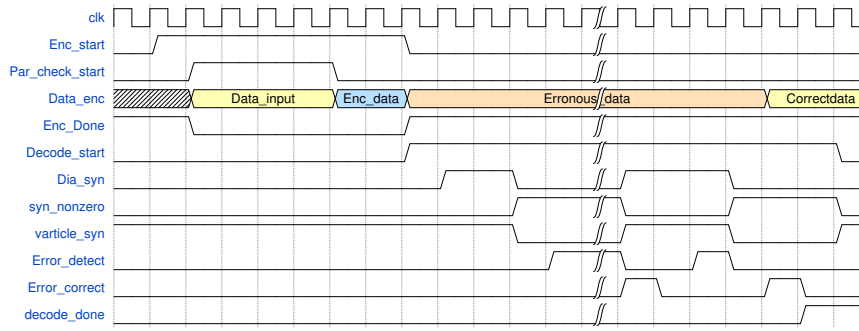


Fig. 4. Timing diagram of different signal used during fault correction

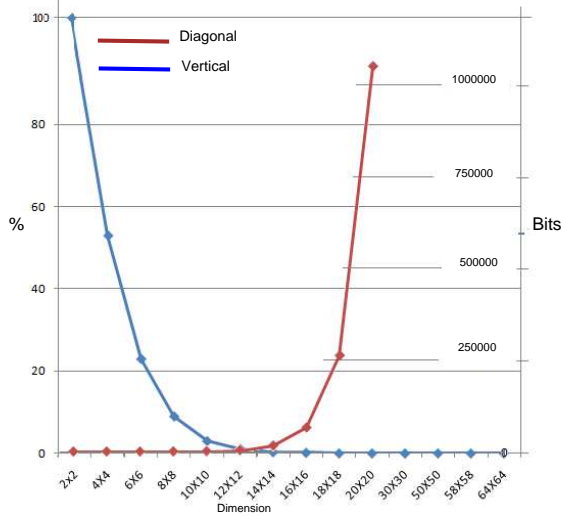


Fig. 5. Error Correcting Efficiency

read back data, ACPC hardware will blindly put the correct value in that bit position. This will increase error correcting capability of the ACPC hardware. Resource utilization, power consumption and critical time of both encoder and decoder are shown in Table II. The result shows that our proposed encoder and decoder consumes very less resource and power compared to the standard application algorithms like Gaussian filter and RC4. Error correcting capability of our proposed code is shown with a graph in Figure 5 where brown line shows number of error bit corrections in successive diagonals and blue line shows fault correcting efficiency of each column. The graph implies that the brown line increases rapidly and blue line decreases drastically as window size (*i.e* dimension of M1 and M2) increases.

VI. CONCLUSION

In this work, we have proposed one new ACPC code to protect FPGA from soft error. The proposed code will use less redundant bit compared to the other existing conventional error correcting codes like RS, BCH or turbo to correct the same number of errors. At the same time decoding complexity of this code is very less compared to others. We have also proposed one novel hardware architecture with partial reconfiguration for the hardware implementation of the proposed code. In future we are planning to develop one fault injector emulator to test the error correcting capability of our proposed code.

REFERENCES

[1] H. Nguyen and Y. Yagil, "A systematic approach to ser estimation and solutions," in *Reliability Physics Symposium Proceedings, 2003. 41st Annual. 2003 IEEE International*, March 2003, pp. 60–70.

[2] R. Baumann, "Radiation-induced soft errors in advanced semiconductor technologies," *Device and Materials Reliability, IEEE Transactions on*, vol. 5, no. 3, pp. 305–316, Sept 2005.

[3] G.-H. Asadi and M. Tahoori, "Soft error mitigation for sram-based fpgas," in *VLSI Test Symposium, 2005. Proceedings. 23rd IEEE*, May 2005, pp. 207–212.

[4] S. Golshan and E. Bozorgzadeh, "Single-event-upset (seu) awareness in fpga routing," in *Design Automation Conference, 2007. DAC '07. 44th ACM/IEEE*, June 2007, pp. 330–333.

[5] M. Violante, L. Sterpone, M. Ceschia, D. Bortolato, P. Bernardi, M. Reorda, and A. Paccagnella, "Simulation-based analysis of seu effects in sram-based fpgas," *Nuclear Science, IEEE Transactions on*, vol. 51, no. 6, pp. 3354–3359, Dec 2004.

[6] Xilinx, "Logicore ip soft error mitigation controller v3.4, product guide," 2012.

[7] F. Kastensmidt, L. Sterpone, L. Carro, and M. Reorda, "On the optimal design of triple modular redundancy logic for sram-based fpgas," in *Design, Automation and Test in Europe, 2005. Proceedings*, March 2005, pp. 1290–1295 Vol. 2.

[8] D. P. Siewiorek and R. S. Swarz, *Reliable Computer Systems (3rd Ed.): Design and Evaluation*. Natick, MA, USA: A. K. Peters, Ltd., 1998.

[9] B. Pratt, M. Caffrey, J. Carroll, P. Graham, K. Morgan, and M. Wirthlin, "Fine-grain seu mitigation for fpgas using partial tmr," *Nuclear Science, IEEE Transactions on*, vol. 55, no. 4, pp. 2274–2280, Aug 2008.

[10] S. Manz, J. Gebelein, A. Oancea, H. Engel, and U. Kebschull, "Radiation mitigation efficiency of scrubbing on the fpga based cbm-tof read-out controller," in *Field Programmable Logic and Applications (FPL), 2013 23rd International Conference on*, Sept 2013, pp. 1–6.

[11] I. Herrera-Alzu and M. Lopez-Vallejo, "Self-reference scrubber for tmr systems based on xilinx virtex fpgas," in *PATMOS*, ser. Lecture Notes in Computer Science, J. L. Ayala, B. Garca-Camara, M. Prieto, M. Ruggiero, and G. Sicard, Eds., vol. 6951. Springer, 2011, pp. 133–142. [Online]. Available: <http://dblp.uni-trier.de/db/conf/patmos/patmos2011.html#Herrera-Alzu11>

[12] J. Heiner, B. Sellers, M. Wirthlin, and J. Kalb, "Fpga partial reconfiguration via configuration scrubbing," in *Field Programmable Logic and Applications, 2009. FPL 2009. International Conference on*, Aug 2009, pp. 99–104.

[13] M. D. S. Cristiana Bolchini, Davide Quarta, "Seu mitigation for sram-based fpgas through dynamic partial reconfiguration," in *Proceedings of the 17th ACM Great Lakes symposium on VLSI, GLSVLSI '07*, 2007, pp. 55–60.

[14] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near shannon limit error-correcting coding and decoding: Turbo-codes. 1," in *Communications, 1993. ICC '93 Geneva. Technical Program, Conference Record, IEEE International Conference on*, vol. 2, May 1993, pp. 1064–1070 vol.2.

[15] S. P. Park, D. Lee, and K. Roy, "Soft-error-resilient fpgas using built-in 2-d hamming product code," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 20, no. 2, pp. 248–256, Feb 2012.

[16] E. Ibe, H. Taniguchi, Y. Yahagi, K. Shimbo, and T. Toba, "Impact of scaling on neutron-induced soft error in srams from a 250 nm to a 22 nm design rule," *Electron Devices, IEEE Transactions on*, vol. 57, no. 7, pp. 1527–1538, July 2010.

[17] L. Frigerio, M. Radaelli, and F. Salice, "Convolutional coding for seu

mitigation,” in *Test Symposium, 2008 13th European*, May 2008, pp. 191–196.

- [18] P. Rao, M. Ebrahimi, R. Seyyedi, and M. Tahoori, “Protecting sram-based fpgas against multiple bit upsets using erasure codes,” in *Design Automation Conference (DAC), 2014 51st ACM/EDAC/IEEE*, June 2014, pp. 1–6.
- [19] A. M. Patel, “Adaptive cross-parity (axp) code for a high-density magnetic tape subsystem,” *IBM Journal of Research and Development*, vol. 29, no. 6, pp. 546–562, Nov 1985.

This figure "flow.jpeg" is available in "jpeg" format from:

<http://arxiv.org/ps/1509.06891v1>

This figure "graph.png" is available in "png" format from:

<http://arxiv.org/ps/1509.06891v1>